



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/782,309	02/19/2004	Ari Juels	4414-35	7635

7590 02/10/2005

Ryan, Mason & Lewis, LLP  
90 Forest Avenue  
Locust Valley, NY 11560

EXAMINER

BANGACHON, WILLIAM L

ART UNIT PAPER NUMBER

2635

DATE MAILED: 02/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

10/782,309

Applicant(s)

JUELS, ARI

Examiner

William Bangachon

Art Unit

2635

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 19 February 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-33 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 17-19, 21 and 22 is/are allowed.
- 6) ☒ Claim(s) 1-16, 20, 23-33 is/are rejected.
- 7) ☒ Claim(s) 17-19, 21 and 22 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 19 February 2004 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 2/19/04.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

## **DETAILED ACTION**

### ***Drawings***

1. The drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, the “verifier, which is other than the reader” must be shown or the feature(s) canceled from the claim(s). No new matter should be entered.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as “amended.” If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled “Replacement Sheet” in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the examiner does not accept the changes, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

***Claim Rejections - 35 USC § 103***

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

4. Claims 1-2, 4-8, 20, 23-25, 30, and 32-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over USP 6,842,106 (Hughes et al) in view of USP 4,928,098 (Dannhaeuser).

In claims 1 and 2, Hughes teach of a method for use in an RFID system comprising at least one or more tags 44 (RFID device) and at least one or more reader/s (32) which communicates with the tag {abstract}, the method comprising the steps of:

associating a plurality of pseudonyms (key value) with the tag (RFID device) {col. 5, lines 47-50; col. 6, lines 32-33, lines 64-65; col. 7, lines 51-53}; and

transmitting from the tag (RFID device) pseudonyms in response to different reader queries of the RFID device {col. 6, lines 15-18, lines 27-28}. In this case, the pseudonyms are converted to pseudo random number based on the key value {col. 6, lines 18-26};

wherein an authenticator (authorized verifier) is able to determine that the different transmitted pseudonyms (key value) are associated with the same tag {col. 5, lines 61-64; col. 6, lines 42-46}. In this case, the reader doubles as an authenticator {col. 6, lines 16-18}.

Although Hughes teaches of using multiple key values {col. 7, lines 52-58}, Hughes does not disclose expressly "transmitting different ones of the pseudonyms". Dannhaeuser, in the same field of endeavor (wireless communication), teach of storing plurality of pseudonyms in tabular form in both a transmitter and receiver (as shown in the table of column 3) wherein the plurality of pseudonyms are cyclically traversed by the transmitter and receiver during transmission {Dannhaeuser, col. 3, lines 1+}. Dannhaeuser teaches that this feature foils attempts of code grabbers from copying and re-using a single transmitted pseudonym to be used in unauthorized accesses {Dannhaeuser, col. 1, lines 26+}. Hughes is concerned with communication security {Hughes, col. 2, lines 29+}. Clearly, the teaching of Dannhaeuser is desirable in the system of Hughes. Therefore, at the time of the invention, it would have been obvious to one of ordinary skill in the art to be transmitting different ones of the pseudonyms in the system of Hughes, as taught by Dannhaeuser, because it provides security to a

Art Unit: 2635

wireless communication by foiling attempts of code grabbers from copying and re-using a single transmitted pseudonym to be used in unauthorized accesses.

In claims 4, the tag is configured to authenticate itself to an authenticator only after the authenticator has authenticated itself to the tag {Hughes, col. 7, lines 32-47}.

In claim 5, the authenticator authenticates itself to the tag by releasing to the tag a first challenge value (authentication value) unique to a given pseudonym transmitted by the tag {Hughes, col. 7, lines 16-23}.

In claim 6, the tag authenticates itself to the authenticator by releasing to the authenticator a second challenge value (authentication value) unique to a given pseudonym transmitted by the RFID device {Hughes, col. 7, lines 24-31}.

In claim 7, one or more of the pseudonyms each comprise an identifier of the tag {Hughes, col. 6, lines 57-65}. In this case, the tag key value identifies the tag.

In claim 8, the method of claim 1 wherein one or more of the pseudonyms each comprise a portion of an identifier of the RFID device {Hughes, col. 6, lines 60-62}. In this case, the tag key value is convoluted to obscure the key value.

In claim 20, a verifier is configured to store for a given RFID device Tx an address no. (a static identifier idx) corresponding to at least one pseudonym of Tx {Dannhaeuser, Fig. 3}.

In claim 23, a verifier specifies value identifying a particular pseudonym {Dannhaeuser, col. 3, lines 49+}.

In claim 24, the RFID device determines which of the plurality of pseudonyms to transmit responsive to a given reader query based at least in part on timing information {Dannhaeuser, paragraph bridging cols. 3 and 4}.

In claim 25, the method of claim 1 wherein the RFID device incorporates a pseudorandom number generator, where  $fx(i)$  represents an output of the pseudorandom number generator for index  $i$ , where  $x$  is a key value (seed) associated with the RFID device {Hughes, col. 5, lines 53-64}.

Claims 30 and 32 recites a system/apparatus for practicing the method of claim 1 and therefore rejected for the same reasons.

Claim 33 recites the limitations of claim 1 and therefore rejected for the same reasons, further comprising determining utilizing an updateable set of one-time pads (index designators) maintained in the device {Dannhaeuser, col. 4, lines 5-24}.

5. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over USP 6,842,106 (Hughes et al) in view of USP 4,928,098 (Dannhaeuser), and further in view of USP 6,724,895 (Turner et al).

In claim 3, Hughes does not disclose expressly "the transmitted pseudonyms are authenticated by an authenticator (verifier) other than the reader". Turner, in the same field of endeavor, teaches of having a plurality of readers/verifiers in an RFID system {col. 4, lines 40-42}. Clearly, since a verifier is also a reader, anyone of them is the reader and anyone of them is the verifier {Turner, Figure 1}. And since the reader of Hughes is also an authenticator {Hughes, col. 6, lines, 15-16}, a plurality of readers in the system of Hughes, as evidenced by Turner, would have an authenticator authenticating the transmitted pseudonym that is other than the reader. Therefore, at the time of the invention, it would have been obvious to one of ordinary skill in the art to have a plurality of readers in the system of Hughes, as evidenced by Turner, wherein an authenticator authenticates the transmitted pseudonym that is other than the reader.

6. Claims 9-16, 14-16, and 26-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over USP 6,842,106 (Hughes et al) in view of USP 4,928,098 (Dannhaeuser), and further in view of USP 6,225,889 (Furuta et al).



In claims 9-16, although Hughes in view of Dannhaeuser teach that the pseudonyms (key values) are stored in the RFID device as an ordered list of pseudonyms {Hughes, col. 7, lines 52-53; Dannhaeuser, Fig. 3}, Hughes does not disclose expressly "the step of designating a particular one of the pseudonyms as a current pseudonym and, in response to a given reader query, transmitting the current pseudonym, wherein over a plurality of reader queries the pseudonym designated as the current pseudonym periodically cycles through the list of pseudonyms". Furuta et al, in the same field of endeavor (transponder systems), teach of a method of producing rolling codes between a vehicle transceiver 2 (analogous to the claimed reader) and key transceiver 1 (analogous to the claimed RFID device). The rolling codes are constantly changed by cycling through a different one of a plurality of initial code variables (pseudonym) stored in the memory (5) of the vehicle transceiver 2, shown in Figure 3 {Furuta, col. 5, lines 13-26}. Initially, one of the plurality of the initial code variable stored in the memory (5) of the vehicle transceiver 2 is designated as the current initial code variable, transmitted to the RFID device and stored in the memory of the RFID device (as claimed in 10 and 12) {Furuta, col. 4, lines 17-29}. So that in response to an as needed initial reader query (as claimed in 11), the current initial code variable stored in the memory of the RFID device is used to produce a unique rolling code {Furuta, col. 6, lines 53+} and transmitted to the reader {Furuta, col. 7, lines 11+}. In the case of a mismatched determination, a given period of time is given to a user to transmit another rolling code (as claimed in 13) {Furuta, col. 8, lines 4-11}. Obviously, these features are

Art Unit: 2635

desirable in the system of Hughes because it provides a high degree of security without compromising system cost, to one of ordinary skill in the art.

In claims 14-16, the initial code variable may be altered sequentially (as claimed in 14) by the reader {Furuta, col. 8, lines 60+}, in response to receipt of refresh information (as claimed in 15) {Furuta, col. 8, lines 18-22}, after the current initial code variable is determined to be invalid (as claimed in 16) {Furuta, col. 7, lines 63+}. Furuta et al teach that the method above is capable of producing rolling codes with a high degree of security using a simple algorithm that do not require large storage capacity {Furuta, col. 1, lines 61-65}. Hughes is concerned with tradeoffs between level of security and system cost {Hughes, col. 7, lines 1-3}. Obviously, these features are desirable in the system of Hughes because it provides a high degree of security without compromising system cost, to one of ordinary skill in the art.

In claim 26, the method of claim 25 wherein the RFID device generates the plurality of pseudonyms as pseudonyms  $c1 = f(1)$ ,  $c2 = f(2)$ , ...,  $ck = f(3)$  {Furuta, col. 8, lines 60-65}.

In claim 27, the method of claim 25 wherein the RFID device and a verifier of the system attempt to maintain a common counter  $dx$  unique to the RFID device, and share the seed  $n$  {Hughes, col. 5, lines 46-50}.

In claim 28, the method of claim 27 wherein in order to determine which RFID device is associated with a given incoming value  $g$ , the verifier performs a lookup in a list  $\{f_x(dx)\}$  of current  $g$  values for a plurality of RFID devices {Hughes, col. 5, lines 21-23}. In this case,  $g$ =tag identification code. And since there is a plurality of tags {Hughes, col. 5, lines 8-10}, obviously, a list of identification code for each tag is stored in the memory of the authenticator to distinguish which tag has responded to an interrogation signal, to one of ordinary skill in the art.

In claim 29, the method of claim 27 wherein for a given counter value  $d$ , the RFID device computes  $cd=f(bk + d)$ , where  $b$  denotes a base value, and the verifier provides a subsequent instruction to the RFID device to increment the base value  $b$  {Furuta, col. 6, lines 48-52}.

***Allowable Subject Matter***

7. Claims 17-19 and 21-22 are allowed.
8. The following is a statement of reasons for the indication of allowable subject matter:

With regards to claims 17-19 in combination with claim 1, the cited prior art do not disclose the use of one-time pads as claimed.

With regards to claims 21-22 in combination with claims 1 and 20, the cited prior art do not disclose encrypting  $idx || zx$  under a symmetric key  $K_a$ , as claimed.

9. Claims 17-19 and 21-22 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

***Examiner Contact Information***

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to William Bangachon whose telephone number is (571)-272-3065. The examiner can normally be reached on 4/4/10.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael Horabik can be reached on (571)-272-3068. The fax phone numbers for the organization where this application or proceeding is assigned is 703-872-9314 for regular and After Final formal communications. The examiner's fax number is (571)-273-3065 for informal communications.

Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Art Unit: 2635

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-4700.

William L Bangachon  
Examiner  
Art Unit 2635

February 3, 2005

MICHAEL HORABIK  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2600  
